,RESEARCH ARTICLE OPEN ACCESS

IMAGE AUTHENTICATION

NeerajSinghRathod MangeshRohankar ,VarshaAmbule
1(Information Technology, Smt. RadhikataiPandav College, Nagpur
Email: neerajsinghrathod@gmail.com)
2 (Information Technology, Smt. RadhikataiPandav College, Nagpur
Email:m2211rohankar@gmail.com)
3 (Information Technology, Smt. RadhikataiPandav College, Nagpur
Email:varsha.var53@gmail.com)

Abstract:

Now a days the transmission and distribution of the digital images by appending the digital signatures and content based image authentication schemes facing some triggers which are suitable for the insecure network and robust to transmission errors.To meet this need, a content-based image authentication scheme that is suitable for an insecure network and robust to transmission errors is proposed. The proposed scheme exploits the scalability of a structural digital signature in order to achieve a good tradeoff between security and image transfer for networked image applications. In this scheme, multi scale features are used to make digital signatures robust to image degradations and key dependent parametric wavelet filters are employed to improve the security against forgery attacks. This scheme is also able to distinguish tampering areas in the attacked image. Experimental results show the robustness and validity of the proposed scheme.

Keyword: **Transmission, digital image, digital signature authentication schemes.**

Introduction

Digital images have been widely used in ourcommunity. Such massive amount digital images have been recently applied in forensic science, such as we can figure out features of suspects or characteristic marks of criminal vehicles. However, with proper computer software, we can modify or duplicate those image data easily. If those modification or duplication is unauthorized, it will make us doubtful when submitting digital images as evidence in court.

Nevertheless, those documents and records still cannot prohibit the malicious or criminal obfuscation from altering the content of the digital evidence effectively and completely. Therefore, in order to assist the examination and analysis of digital image evidence by forensic examiners in the laboratory, we propose a robust and convenient technology to improve this situation. The technology is based on cryptography and effectively enhances the strength of power of evidence. The proposed technology creates a unique code as a ‘fingerprint’or ‘digital signature’ to be with an image. Therefore, we can easily figure out if anyone tampers with the evidence content.

In cryptography, one of the techniques to produce a message authentication code is based on using hash functions. A hash function provides additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and meddage integrity. Hash functions are widely used to protect password contents and interactive authentication in the internet. Even a single bit changedin the input message, though, will produce a different hash value. In this paper, we apply this important property to provide integrity protection

Literature Survey

In this paper, we apply this important property to provide integrity protection.Recent advances in networking and digital media technologies have created a large number of networked multimedia applications. Those applications are often deployed in a distributed network environment that makes multimedia contents vulnerable to privacy and malicious attacks. For insecure environments, it is possible for an enemy to tamper with images during transmission. To guarantee trustworthiness, image authentication techniques have emerged to confirm content integrity and prevent forgery. These techniques are required to be robust against normal image processing and transmission errors, while being able to detect malevolent tampering on the image.

Such authentication techniques have wide applicability in law, commerce, journalism and national defense. Image content in compact representation . It is stored as an extra file and later

used for authentication. Signature-based methods can work on both the integrity protection of the image and repudiation prevention of the sender. Watermarking, on the other hand, is an invasive Method that really embeds a message into an image data and the hidden message is later extracted to verify the authenticity of image content .

Watermark-based approaches only work for protecting the integrity of the image. The major difference between a watermark and a digital signature is that the embedding process of the former requires the content of the media to change. As users no longer physically possess the storage oftheir data, traditional cryptographic primitives for the purpose of data security protection cannot be directlyadopted . In particular, simply downloading allthe data for its integrity verification is not a practicalsolution due to the expensiveness in I/O and transmissioncost across the network.

Besides, it is ofteninsufficient to detect the data corruption only whenaccessing the data, as it does not give users correctnessassurance for those unaccessed data and might be too late to recover the data loss or damage. Consideringthe large size of the outsourced data and the user'sconstrained resource capability, the tasks of auditing the data correctness in a environment can beformidable and expensive for the cloud users. Moreover, the overhead of using storageshould be minimized as much as possible, such thatuser does not need to perform too many operationsto use the data (in additional to retrieving the data).

For example, it is desirable that users do not need toworry about the need to verify the integrity of the databefore or after the data retrieval. Besides, there may bemore than one user accesses the same Network storage,say in an enterprise setting. For easier management,it is desirable that the cloud server only entertainsverification request from a single designated party. Therefore, how to enable a privacy-preservingthird-party auditing protocol, independent to dataencryption, is the problem we are going to tacklein this paper. Our work is among the first fewones to support privacy-preserving public auditing in Network, with a focus on data storage.

Related Work

Existing methods with Content-Based Digital Signature Authentication will assume reliable noise-free transport. These methods do not work well when used to transmit images over the error-prone wireless channel. For example, any transmission bit error will render traditional authentication a failure. It is clear that traditional authentication algorithms do not cope well with loss networks and the losstolerant nature of the multimedia data.

The Proposed method The Image Authentication over Wireless Networks. Here requires careful design of the authentication methodology. It Overcome all issues that we discussed above. The proposed scheme generates only one fixed-length digital signature per image regardless of the image size and the packet loss during transmission.In this scheme, multi-scale features are used to make digital signatures robust to image degradations and key dependent parametricwavelet filters are employed to improve the security against forgery attacks. Visual hashing scheme usually relies on a techniquefor feature extraction as the initial processing stage. Subsequently, the features are further processedto increase robustness and/or reduce dimensionality.To ensure the security of the algorithms, its featuresare required to be key-dependent and must not becomputable without the knowledge of the key usedfor hash construction

Software Requirement

The **Microsoft .NET Framework** is a software technology that is available with several Microsoft Windows operating systems. It includes a large library of pre-coded solutions to common programming problems and a virtual machine that manages the execution of programs written specifically for the framework. The .NET Framework is a key Microsoft offering and is intended to be used by most new applications created for the Windows platform.

The pre-coded solutions that form the framework's Base Class Library cover a large range of programming needs in a number of areas, including user interface, data access, database connectivity, cryptography, web application development, numericalgorithms, and network communications. The class library is used by programmers, who combine it with their own code to produce applications.

Programs written for the .NET Framework execute in a software environment that manages the program's runtime requirements. Also part of the .NET Framework, this runtime environment is known as the Common Language Runtime (CLR). The CLR provides the appearance of an application virtual machine so that programmers need not consider the capabilities of the specific CPU that will execute the program. The CLR also provides other important services such as security, memory management, and exception handling. The class library and the CLR together compose the .NET Framework.

Principal design features:

Common Runtime Engine

The Common Language Runtime (CLR) is the virtual machine component of the .NET framework. All .NET programs execute under the supervision of the CLR, guaranteeing certain properties and behaviors in the areas of memory management, security, and exception handling.

Base Class Library

The Base Class Library (BCL), part of the Framework Class Library (FCL), is a library of functionality available to all languages using the .NET Framework. The BCL provides classes which encapsulate a number of common functions, including file reading and writing, graphic rendering, database interaction and XML document manipulation.

Simplified Deployment

Installation of computer software must be carefully managed to ensure that it does not interfere with previously installed software, and that it conforms to security requirements. The .NET framework includes design features and tools that help address these requirements.

Security

The design is meant to address some of the vulnerabilities, such as buffer overflows, that have been exploited by malicious software. Additionally, .NET provides a common security model for all applications.

Common Language Infrastructure

The core aspects of the **.NET framework** lie within the Common Language Infrastructure, or **CLI**. The purpose of the CLI is to provide a language-neutral platform for application development and execution, including functions for exception handling, garbage collection, security, and interoperability. Microsoft's implementation of the CLI is called the **Common Language Runtime** or **CLR**.

Assemblies

The intermediate CIL code is housed in .NET assemblies. As mandated by specification, assemblies are stored in the Portable Executable (PE) format, common on the Windows platform for all DLL and EXE files. The assembly consists of one or more files, one of which must contain the manifest, which has the metadata for the assembly. The complete name of an assembly (not to be confused with the filename on disk) contains its simple text name, version number, culture, and public key token. The public key token is a unique hash generated when the assembly is compiled, thus two assemblies with the same public key token are guaranteed to be identical from the point of view of the framework. A private key can also be specified known only to the creator of the assembly and can be used for strong naming and to guarantee that the assembly is from the same author when a new version of the assembly is compiled (required to add an assembly to the Global Assembly Cache).

Metadata

All CLI is self-describing through .NET metadata. The CLR checks the metadata to ensure that the correct method is called. Metadata is usually generated by language compilers but developers can create their own metadata through custom attributes. Metadata contains information about the assembly, and is also used to implement the reflective programming capabilities of .NET Framework.

ASP.NET

SERVER APPLICATION DEVELOPMENT

Server-side applications in the managed world are implemented through runtime hosts. Unmanaged applications host the common language runtime, which allows your custom managed code to control the behavior of the server. This model provides you with all the features of the common language runtime and class library while gaining the performance and scalability of the host server.

The following illustration shows a basic network schema with managed code running in different server environments. Servers such as IIS and SQL Server can perform standard operations while your application logic executes through the managed code.

C#.NET

ADO.NET OVERVIEW

ADO.NET is an evolution of the ADO data access model that directly addresses user requirements for developing scalable applications. It was designed specifically for the web with scalability, statelessness, and XML in mind.

ADO.NET uses some ADO objects, such as the **Connection** and **Command** objects, and also introduces new objects. Key new ADO.NET objects include the **Dataset**, **Data Reader**, and **Data Adapter**.

The important distinction between this evolved stage of ADO.NET and previous data architectures is that there exists an object -- the **DataSet** -- that is separate and distinct from any data stores. Because of that, the **DataSet** functions as a standalone entity. You can think of the DataSet as an always disconnected recordset that knows nothing about the source or destination of the data it contains. Inside a **DataSet**, much like in a database, there are tables, columns, relationships, constraints, views, and so forth.

SQL SERVER -2008

A database management, or DBMS, gives the user access to their data and helps them transform the data into information. Such database management systems include dBase, paradox, IMS, SQL Server and SQL Server. These systems allow users to create, update and extract information from their database.

A database is a structured collection of data. Data refers to the characteristics of people, things and events. SQL Server stores each data item in its own fields. In SQL Server, the fields relating to a particular person, thing or event are bundled together to form a single complete unit of data, called a record (it can also be referred to as raw or an occurrence). Each record is made up of a number of fields. No two fields in a record can have the same field name.

During an SQL Server Database design project, the analysis of your business needs identifies all the fields or attributes of interest. If your business needs change over time, you define any additional fields or change the definition of existing fields.

System Architecture

There are three basic elements in any encryption

system:
-- a means of changing information into code (the algorithm);
-- a secret starting point for the algorithm (the key); and
-- a system to control the key (key management).

The key determines how the algorithm - the encryption process - will be applied to a particular message, and matching keys must be used to encrypt and decrypt messages.

The algorithm used in an encryption system normally remains the same for the life of the equipment, so it is necessary to change keys frequently in order that identical encryption is not applied to messages for a long period. It is generally desirable to change the keys on an irregular but managed basis. Key management deals with the generation, storage, distribution, selection, destruction and archiving of the key variables. Two basic types of encryption in use today are known as private key (also called single or symmetrical key) encryption and public (or asymmetrical) key encryption.

Private-Key-Encryption

In private key encryption, the same key is used for both encryption and decryption. The key must be kept secret so that unauthorized parties cannot, even with knowledge of the algorithm, complete the decryption process. A person trying to share encrypted information with another person has to solve the problem of communicating the encryption key without compromising it. This is normally achieved by programming keys into all encrypts prior to deployment, and the keys should be stored securely within the devices. In a relatively small network of encrypts, the task of key management (including key changes) is easily handled for a private key system. Private key encryption is a commonly used method of key management, and is used for standard algorithms such as DES and Triple DES.

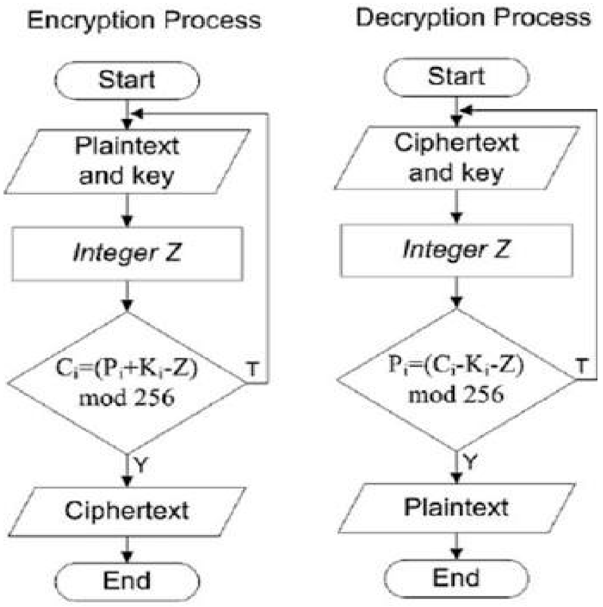

Fig – Encryption And Decryption Process

Public Key Encryption

Public key encryption solves the problem of maintaining key security by having separate keys for encryption and decryption, which uniquely match each other but are not predictable from each other. The user retains a private decryption key and makes the public key available for use by anyone interested in sending the user sensitive information. The relationship between the keys is such that given the public key a person cannot easily derive the private key.

Senders use the recipient's public key to send encrypted messages. Recipients use their corresponding private key to decrypt messages. The private key can also be used to encrypt messages, which can be decrypted by anyone with knowledge of the public key (the purpose of this is to provide verification of the origin rather than to achieve secrecy). Public key encryption is relatively inefficient and is not suitable for either encrypting large volumes or operating at high speeds. The RSA algorithm is a well-known form of public key encryption.

The main purpose for preparing this document is to give a general insight into the analysis and requirements of the existing system or situation and for determining the operating characteristics of the system.

The digital signature and watermarking methodsare used for image authentication. Digital signature encodesthe signature in a file separate from the original image.Cryptographic algorithms have suggested severaladvantages over the traditional encryption algorithms suchas high security, speed, reasonable computationaloverheads and computational power. A digital watermarkand signature method for image authentication is usingcryptography analysis.

The digital signature created for the originalimage and apply watermark. Images are resized beforetransmission in the network. After digital signature andwater marking an image, apply the encryption anddecryption process to an image for the authentication. Theencryption is used to securely transmit data in opennetworks for the encryption of an image using public keyand decrypt that image using private key.Digital signature is a sort of Cryptography.

Cryptography means keeping communications private. Itsmainly used for the converting of the information isencryption and decryption. No one can't access theinformation without access key. The main process of the digital signature is similarly as the handwritten signatureand it's like paper signature and it having the digitalcertificate using this verifies the identity.

Watermarking is a sub-discipline of informationhiding. It is the process of embedding information into adigital signal in a way that is difficult to remove. It'sproviding copyright protection for intellectual methodthat's in digital format.The cryptography is providing better mechanismsfor information security. In this analysis to provide thepublic and private keys for recovery the originalinformation. The ability store and transfer sensitiveinformation. By using the different encryption methods forgenerating public keys, decryption using for private keys.

This method applied to digital signatures and watermarking for to provide high security in transactions.In the image authentication procedure shown in Fig.4, given corrupted images by transmission and theirassociated digital signatures . The proposedscheme authenticates both the integrity and thesource of the received image by applying thefollowing process on the image in the followingorder: (1) perform content-adaptive errorconcealment, if some blocks are damaged; (2) extractthe SDS of the received image using the samemethod used in image signing; (3) decrypt thesignature by using the sender's public key; (4) perform a content authenticity verification procedureusing both the decrypted signature and the extractedone to calculate the degree of authenticity.

Hash Functions

Hash functions [ ], H (M), have been used incomputer science and information security for a longtime. They compress an arbitrary-length input, M, toa string of small and fixed length arbitrarily whichgenerally called hash value (message digest), h, canreplace the authenticity of a large amount of information(message) by the authenticity of a much smaller hashvalue. The hash value is a set of a short string of randomlookingletters and numbers.

$$\boxed{h=H(M)}$$

A hash function must have the following properties:
1. H can be performed to any block of data in any size.
2. H produces a small and fixed length of output.
3. For any generated h, it is computationally infeasibleto find any M to conform that H (M) =h inmathematics. (One-way property)
4. For any input, M, it is computationally infeasible tofind M'to conform that H (M) =H (M□).

5. For any pair (M, M'), it is infeasible to find H (M)

=H (M') in mathematics.

The third property is the "one-way property".That means the function works in one direction and it'snearly impossible to derive the original text from thestring. A one-way hash function is used to create digitalsignatures, which in turn identify and authenticate thesender and message of a digitally distributed message(hence the name one-way). A good one-way hashfunction is also collision-free. That means it is hard tocreate two inputs with the same hash value.

Modules:

This system is divided into Four modules:

- Network module.
- Encryption module.
- Decryption module.
- Authentication module

1.Network module:

This module is both accessed by sender and receiver in order to establish a wireless channel between them. During this process sender identifies the address of receiver. This module support following services:

- Finding IP address.
- Establish connection.

2.Encryption module:

This module is accessed by sender at the location of sender side and its objective is to encrypt the plain text data given by sender. The encryption can be done either private or public keys or using water marking methods or combination it support following services:

- Get input data.
- Generate private or public key.
- Select image
- Encrypt using keys.
- Encrypt by hiding data behind the image.

3.Decryption module:

This module accessed by the receiver at receiver location and its objective is to copy decrypt the encrypted data to original form. During process it follows services:

- Receive encrypted data.
- Generate private or public key.
- Decrypt by using keys.
- Decrypt by extracting data from image

Authentication module:

This is accessed by both sender and receiver. The objective of this module is the sender authenticate, encrypt data, receiver also authenticate encrypted data. So the sender ensures that data is received only by receiver.

Scope of Problem

Scope: This Document plays a vital role in the development life cycle (SDLC)

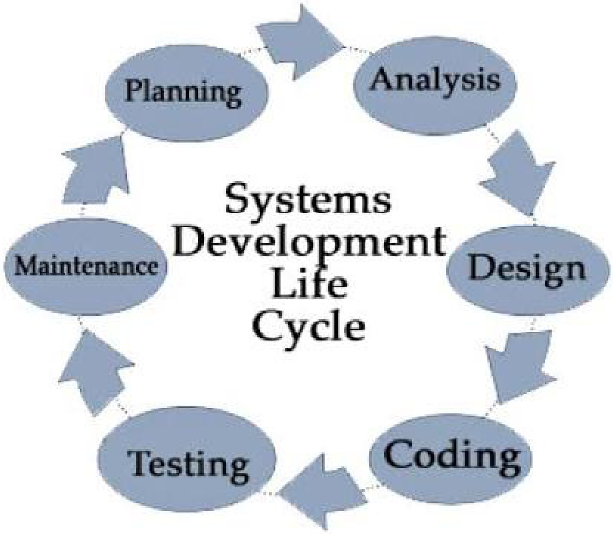

Fig.- System Development life cycle

It describes the complete requirement of the system. It is meant for use by the developers and will be the basic during testing phase. Any changes made to the requirements in the future will have to go through formal change approval process.

Encryption of data plays a vital role in the real time environment to keep the data out of reach of unauthorized people, such that it is not altered and tampered. The digital Encryption System is software, which tries to alter the originality of the text into some encrypted form.

The major task of the Digital Encryption System is to provide the user the flexibility of passing the information implementing the encryption standards as per the specification and algorithms proposed and store the information in a form that is unreadable. The Application should have a reversal process as of which should be in a position to decrypt the data to its original format upon the proper request by the user. While the Encryption and Decryption is done the application should confirm the standards of authentication and authorization of the user.

DES Encrypts and decrypts data in 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher.

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman introduced a cryptographic algorithm.

Each user has their own encryption and decryption procedures, E and D, with the former in the public and the latter kept secret. These procedures are related to the keys, which, in RSA specially, aresets of two special numbers. We of course start out with the message itself, symbolized by M, which is tobe \encrypted". There are four procedures that are specie and essential to a public-key cryptosystem:

a) Deciphering an enciphered message gives you the original message, specially
D(E(M)) = M : (1)

b) Reversing the procedures still returns M:
E(D(M)) = M : (2)

c) E and D are easy to compute.

d) The publicity of E does not compromise the secrecy of D, meaning you cannot easily figure outD from E.

With a given E, we are still not given anclient way of computing D. If C = E(M) is the cipher text, then trying to figure out D by trying to satisfy an M in E(M) = C is unreasonably difficult: the numberof messages to test would be impractically large.
An E that satisfies (a), (c), and (d) is called a \trap-door one-way function" and is also a \trap-doorone-way permutation". It is a trap door because since it's inverse D is easy to compute if certain \trap-door" information is available, but otherwise hard. It is one-way because it is easy to compute in onedirection, but hard in the other. It is a permutation because it satisfies (b), meaning every ciphertext isa potential message, and every message is a ciphertext of some other message. Statement (b) is in factjust needed to provide \signatures".
Now we turn to specific keys, and imagine users A and B (Alice and Bob) on a two-user public-keycryptosystem, with their keys: EA, EB, DA, DB.

This project “DES (Digital Encryption System)” is developed on client server technology. The client encrypts the file and sends to the server. Other client will receive the file and decrypts the file by using the same private key

Conclusion

In this paper, a modified digital signature scheme for image authentication has been proposed. Content-dependent structural image features and wavelet filter parameterization are incorporated into the traditional crypto signature scheme to enhance the system robustness and security. Because the proposed scheme does not require any computational overhead, it is especially suited for wireless authentication systems and other real-time applications.

The analysis and the experimental results confirm that the proposed scheme can achieve good robustness against transmission errors and some acceptable manipulation operations. The scheme is very robust to cutting and pasting counterfeiting attacks. It is also able to tolerate various common image processing manipulations, at the cost of only extra payload introduced into the channel by associating the signature with the image. Further work will conduct more tests on the quality of degraded images.

References

[1]'Digital Signature-Based Image Authentication', in LU C.S. (EDS.): 'Multimedia security: steganography and digital watermarking techniques for protection of intellectual property' (Idea Group Inc., 2003)

[2] SEITZ J.: 'Digital watermarking for digital media' (Idea Group Publishing, 2005).

[3] SCHNEIDER M., CHANG S.-F.: 'A content based digital signature for image authentication'. Proc. IEEE Int. Conf. Image Processing (ICIP'96), 1996.

[4] ANTHONY T., HO S., YONG L.G.: 'Image content authentication using pinned sine transform', EURASIP J. Appl. Signal Process., 2004, 14, pp. 2174 – 2184

[5] LU C.S.: 'On the security of structural information extraction/embedding for image authentication'. Proc. IEEE ISCAS'04, 2004,

[6] SUN Q., HE D., YE S.: 'Feature selection for semi fragile signature based authentication systems'. Proc. IEEE Workshop on Image Signal Processing, 2003,

[7] LIN C.-Y., CHANG S.-F.: 'A robust image authentication method distinguishing JPEG compression from malicious manipulation', IEEE Trans. Circuits Syst. Video Technol., 2001

[8] YE S., LIN X., SUN Q.: 'Content-based error detection and concealment for image transmission over wireless channel'. Proc. IEEE Int. Symp. Circuits and Systems, Thailand, 2003

[9] GINESU G., GIUSTO D.D., ONALI T.: 'Mutual image based authentication framework with JPEG2000 in wireless environment', EURASIP J. Wirel. Commun. Netw., 2006,
2006, pp. 1 – 14 (Article ID 73685)

[10] LIN C.-Y., SOW D., CHANG S.-F.: 'Using self authentication and recovery images for error concealment in wireless environment'. Proc. SPIE ITCom Conf., August 2001

[11] SUN Q., YE S., LIN C.-Y.: 'A crypto signature scheme for image authentication over wireless channel', Int. J. Image Graph., 2005, 5, (1), pp. 1 – 14

[12] YE S., SUN Q., CHANG EE-C.: 'Error resilient content based image authentication over wireless channel'. Proc. IEEE ICIP'06, 2006

[13] KUNDER D., HATZINAKOS D.: 'Digital watermarking using multiresolution wavelet decomposition'. Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Seattle, Washington, 1998

[14] PETER M., UHL M.: 'Watermark security via wavelet filter parametrization'. Proc. Int. Conf. ICASSP, USA, 2000

[15] SWAMINATHAN A., MAO Y., WU M.: 'Robust and secure image hashing', IEEE Trans. Inf. Forensics Sec., 2006, 1, (2),

[16] FRIDRISH J., BALDOZA A.C., SIMARED R.J.: 'Robust digital watermarking based on key dependent basis functions'. Proc. Int. Conf. LNCS:IH, Portland, OR, USA, April 1998, vol. 1525,

[17] LU C.S., LIAO H.M.: 'Structural digital signature for image authentication: an incidental distortion resistant scheme', IEEE Trans. on Multimed., 2003, 5, (2),

[18] YE S., SUN Q., CHANG E.C.: 'Edge directed filter based error concealment for wavelet-based images'. Proc. IEEE Int. Conf. Image Processing, Singapore, 2004

[19] MARTINIAN E., WORNELL G.W., CHEN B.: 'Authentication with distortion criteria', IEEE Trans. Inf. Theory, 2005,